Gesamtskript
Kapitel I
zur Vorlesung
Algebra I

Prof.'in Dr. Salma Kuhlmann

Inhaltsverzeichnis für das Gesamtskript Kapitel 1[1] zur Vorlesung: Algebra I (WiSe2020/2021)

Prof. Dr. Salma Kuhlmann

KAPITEL I: Ringe.

[1] Die Seitenzahlen in Klammern geben die Seitenzahl für die Suche mit Adobe Acrobat Reader an (unter dem Menü ANZEIGE – GEHE ZU – SEITE).

1 Script zur Vorlesung: Algebra 1 (WiSe2020-2021)

Prof. Dr. Salma Kuhlmann

Kurze Einleitung:
Für die Vorlesung Algebra 1 (B3) haben wir vier Kapitel vorgesehen. Das erste Teil besteht aus Kapitel 1 (Ringe) und Kapitel 2 (Körpererweiterungen), das zweite Teil aus Kapitel 3 (Gruppen) und Kapitel 4 (Einführung in die Galoistheorie). In der B4 Vorlesung (Algebra 2 und algebraische Zahlentheorie) werden wir unser Studium von Galois Erweiterungen fortsetzen und vertiefen. Das Vorlesungskalender ist zur Orientierung, und enthält eine voraussichtliche Themenplanung.

Kapitel 1

RINGE

In diesem Kapitel werden wir folgende Ringe und Ringkonstruktionen untersuchen (im Stichwort): Faktorringe, Ringe von Brüchen, Lokalisierungen, Euklidische Ringe, Hauptideal Ringe, Faktorielle Ringe, Polynomringe.
In Skript 1, werden wir zunächst einige Begriffe (die wir schon in Lineare Algebra 1 und 2 gesehen haben) in Erinnerung bringen. Danach werden wir Faktorringe einführen.

§ 1 Erinnerungen

Definition 1.1.
Ein Tripel $(R, +, \cdot)$ ist ein *Ring*, falls R ist eine nichtleere Menge und $+, \cdot$ sind Verknüpfungen auf R so dass: :

- $(R, +)$ ist eine abelsche Gruppe mit neutralem Element $0 \in R$
- Die Verknüpfung $\cdot$ ist assoziativ
- die Distributivitätsgesetze gelten:

Links: $x \cdot (y + z) = (x \cdot y) + (x \cdot z)\ \forall x, y, z \in R$ und

Rechts: $(y + z) \cdot x = (y \cdot x) + (z \cdot x)\ \forall x, y, z \in R$

Definition 1.2.
Ein Ring $(R, +, \cdot)$ ist
(i) *kommutativ* falls $\forall x, y \in R : x \cdot y = y \cdot x$.
(ii) Ein *Ring mit Eins* wenn es existiert $1 \in R$ $(1 \neq 0)$ so dass $\forall x \in R : x \cdot 1 = 1 \cdot x = x$.

In dieser Vorlesung werden wir kommutative Ringe studieren.

Definition 1.3. Sei R ein kommutativer Ring mit 1.

(1) $a \neq 0; a \in R$ ist ein *Nullteiler*, wenn es $b \neq 0; b \in R$ gibt mit $ab = 0$.

(2) R ist ein *Integerring* oder *Integritätsbereich*, wenn er keine Nullteiler hat.

(3) $u \in R$ ist eine *Einheit*, wenn es ein $v \in R$ gibt mit $uv = 1$.

Notation: $R^\times :=$ Menge der Einheiten von R.

Die folgende Begriffe und Beipiele haben wir in LA I und/oder II schon studiert, wir wiederholen die Aussagen, jedoch nicht die Beweise.

Proposition 1.4.
$R^\times$ ist eine multiplikative Gruppe.

Beispiel 1.5.
Wir bezeichnen $\mathbb{Z}_n^\times$ mit $U(n)$

Es gilt: $a \in U(n) \Leftrightarrow \text{ggT}\ (a, n) = 1$.

Die Euler φ-Funktion $\varphi : \mathbb{N} \to \mathbb{N}$ wird so definiert: $\varphi(n) := \mid U(n) \mid$.

Siehe Übungsblatt für eine ausführliche Ausarbeitung der Eigenschaften von φ:

(1) $\varphi(p^v) = p^v - p^{v-1}$ für p Primzahl und $v \in \mathbb{N}$

(2) φ ist eine multiplikative arithmetische Funktion i.e. $\varphi(ab) = \varphi(a)\varphi(b)$, wenn $\text{ggT}\ (a, b) = 1$.

Definition 1.6.

(1) $S \subseteq R$ ist ein *Teilring*, wenn $S \neq \varnothing; a, b \in S \Rightarrow a - b \in S$ und $ab \in S$.

(2) Seien R, S kommutative Ringe (mit 1_R und 1_S).
Eine Abbildung $\varphi : R \to S$ ist ein *Ringhomomorphismus*, wenn
$\varphi(1_R) = 1_S, \varphi(a + b) = \varphi(a) + \varphi(b), \varphi(ab) = \varphi(a)\varphi(b)$.

(3) Ein *Ringisomorphismus* ist ein bijektiver Ringhomomorphismus.
Notation: $\varphi : R \simeq S$ oder $R \overset{\varphi}{\simeq} S$ oder $R \simeq S$.

Notation:
$\ker \varphi := \{x \in R; \varphi(x) = 0\}$
$\text{im}\ \varphi := \{y \in S; \exists x \in R \text{ mit } \varphi(x) = y\} := \varphi(R)$.

Bemerkung 1.7.
Sei φ ein Homomorphismus: φ ist injektiv $\Leftrightarrow \ker \varphi = \{0\}$.

Beispiel 1.8.
Sei $n \in \mathbb{N}$
$a \in \mathbb{Z}; \overline{a} :=$ Rest nach Division durch n.

$$\begin{array}{rccc} \varphi: & \mathbb{Z} & \to & \mathbb{Z}_n \\ & a & \mapsto & \overline{a} \end{array}$$

ist ein Ringhomomorphismus mit $\ker\varphi = \{nz / z \in \mathbb{Z}\} := n\mathbb{Z}$

Definition 1.9.
Ein Teilring $I \subseteq R$ ist ein *Ideal*, wenn aus $r \in R$ und $x \in I$ folgt: $rx \in I$.
Notation: $I \lhd R$

Beispiel 1.10.
$I = R$ und $I = \{0\}$

Terminologie:
$I \lhd R$ und $I \neq R$ heißt *echtes Ideal*.
$I \lhd R$ und $I \neq \{0\}$ heißt *nicht triviales Ideal*.

Proposition 1.11.
Sei $\varphi : R \to S$ ein Ringhomomorphismus. Es gelten:

(1) im φ ist ein Teilring von S.

(2) $\ker\varphi$ ist ein Ideal von R.

Beweis: ÜA.

§ 2 Faktorringe

Sei $I \lhd R$. Wir definieren eine binäre Relation auf R wie folgt:
$\forall x, y \in R : x \sim y \mod I$ genau dann, wenn $x - y \in I$.

Diese ist eine Äquivalenzrelation (siehe Übungsblatt).

Notation:
(i) Für $x \in R$ bezeichnen wir mit $x + I$ die Äquivalenzklasse $[x]$ von x.
(ii) Wir bezeichnen $R/I := \{x + I \mid x \in R\}$ die Menge der *Nebenklassen von R modulo I*.

Proposition 1.12.
R/I ist ein Ring mit den Ringoperationen
$(r + I) + (s + I) := (r + s) + I$ und
$(r + I) \cdot (s + I) := (rs) + I$
für alle $r, s \in R$.

Beweis: siehe Übungsblatt.

Definition 1.13.
R/I ist der *Faktorring* "$R \mod I$".

Satz 1.14. (Isomorphiesatz für Ringe)

(1) Sei $\varphi : R \to S$ ein Ringhomomorphismus. Es gilt $R/\ker\varphi \simeq \text{im}\,\varphi$.

(2) Umgekehrt: Ist $I \lhd R$, dann ist die *kanonische Projektion*

$$\begin{array}{rccc} \pi: & R & \to & R/I \\ & r & \mapsto & r+I \end{array}$$

ein surjektiver Ringhomomorphismus mit $\ker\pi = I$.

Also sind die Ideale genau die Kerne von Ringhomomorphismen.

Beweis:
Setze $I := \ker\varphi$. Wir prüfen unmittelbar dass die Abbildung

$$\begin{array}{rccc} \Phi: & R/I & \twoheadrightarrow & \varphi(R) \\ & x+I & \mapsto & \varphi(x) \end{array}$$

wohldefiniert ist, d.h. $x + I = y + I$ impliziert $\varphi(x) = \varphi(y)$.

Es ist außerdem klar, dass Φ surjektiv und ein Ringhomomorphismus ist (ÜA).

Wir berechnen nun $\ker\Phi$:
$\Phi(x+I) = 0 \Leftrightarrow \varphi(x) = 0 \Leftrightarrow x \in \ker\varphi \Leftrightarrow x \in I \Leftrightarrow x + I = 0 + I$;
somit ist $\ker\Phi = \{0 + I\}$ (das Nullelement der Faktorring R/I).

Es folgt aus Bemerkung 1.7 dass die Abbildung auch injektiv, und damit ein Isomorphismus.

Der Beweis von (2) ist analog. Siehe Übungsblatt. □

Beispiel 1.15.
Betrachte die Abbildung in Beispiel 1.8:

$$\begin{array}{rccc} \varphi: & \mathbb{Z} & \to & \mathbb{Z}_n \\ & a & \mapsto & \overline{a} \end{array}$$

ist ein Ringhomomorphismus mit $\ker\varphi = \{nz / z \in \mathbb{Z}\} := n\mathbb{Z}$

Es folgt nun aus Satz 1.14 dass $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$

Korollar 1.16.
Sei $I \lhd R, J \lhd R$ mit $I \subseteq J$ (insbesondere $I \lhd J$). Dann ist $J/I \lhd R/I$ und $(R/I)/(J/I) \simeq R/J$.

Beweis:
Die Abbildung

$$\begin{array}{rccc} \Phi: & R/I & \twoheadrightarrow & R/J \\ & x+I & \mapsto & x+J \end{array}$$

ist ein surjektiver Ringhomomorphismus mit $\ker\Phi = J/I$. Die Behauptung folgt nun aus Satz 1.14. □

2 Script zur Vorlesung: Algebra 1 (WiSe2020-2021)

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir zunächst eine wichtige Anwendung vom Isomorphiesatz ableiten; in Korollar 2.1 werden die Ideale von einem Faktorring charakterisieren. Dann werden wir verschiedene allgemeine Idealkonstruktionen einführen (beziehungsweise in Erinnerung bringen). Wir werden bei der Gelegenheit das Lemma von Zorn kennenlernen.

Notation:
$x + I$ wird in dieser Vorlesung auch als $\overline{x}$ geschrieben .

Korollar 2.1.
Sei R ein kommutativer Ring und $I \lhd R$. Sei $\mathcal{T} \coloneqq \{A \subseteq R \,;\, I \subseteq A \subseteq R\}$ die Menge der Teilringe von R die I enthalten und $\mathcal{T}_I$ die Menge der Teilringe von R/I. Es gelten für $A \in \mathcal{T}$:

1. $I \lhd A$,
2. Die Abbildung
$$A \mapsto A/I$$
ist eine bijektive, Inklusionserhaltende Korrespondenz zwischen $\mathcal{T}$ und $\mathcal{T}_{\mathcal{I}}$,
3. $A \lhd R$ genau dann, wenn $A/I \lhd R/I$.

Beweis:
Siehe Übungsblatt. □

Definition 2.2.
Sei $A \subseteq R$ eine beliebige Teilmenge. Das *von A erzeugte Ideal*, mit $< A >$ bezeichnet, ist das kleinste Ideal, das A enthält.

Die folgende Aussage ist als ÜA zu prüfen:

Bemerkung 2.3.

1. $< \varnothing >= \{0\}$.
2. $< A >= \bigcap_{\{A \subseteq J \lhd R\}} J$ (der Durchschnitt aller Ideale, die A enthalten).
3. $< A >= \{\sum_{i=1}^{n} r_i a_i \,;\, n \in \mathbb{N} \,,\, r_i \in R \,,\, a_i \in A\}$
(die Menge aller endlichen R-Linearkombinationen aus Elementen von A).

Konvention: Wenn $A = \{a_1, \ldots, a_l\}$ endlich ist, so schreiben wir einfach $< a_1, \ldots, a_l >$.

Definition 2.4.
Sei $a \in R$, $< a >= \{ra; r \in R\}$ heißt *Hauptideal*, das von a erzeugt ist.

Beispiel 2.5.
$< 1 >= R$ und $< 0 >= \{0\}$.

Proposition 2.6.
Seien R ein kommutativer Ring mit 1, und $I \lhd R$. Es gelten:

(1) $I = R$ genau dann, wenn $I \bigcap R^\times \neq \varnothing$

(2) R ist ein Körper genau dann, wenn die einzigen Ideal R und $\{0\}$ sind.

Beweis:

(1) "$\Rightarrow$" trivial

"$\Leftarrow$" $u \in I$ Einheit $\Rightarrow$ $u^{-1}u \in I$ $\Rightarrow$ $1 \in I$

$\uparrow$

$\in R$ $\Rightarrow$ $r.1 \in I \ \forall \ r \in R$

(2) "$\Rightarrow$" Sei $I \neq \{0\}$ und $u \in I; u \neq 0$. Dann ist u eine Einheit und somit $I = R$.

"$\Leftarrow$" Sei $x \in R, x \neq 0$. Dann ist $< x >= R$, d.h. $1 \in < x >$, also existiert ein $r \in R$ mit $rx = 1$, also $r = x^{-1}$ □

Korollar 2.7.
Sei R ein Körper, S ein Ring und $\varphi : R \to S$ ein Ringhomomorphismus. Ist $\varphi \neq 0$, dann ist φ injektiv.

Beweis:
Proposition 1.11(2) liefert dass $\ker \varphi \lhd R$. Da $\ker \varphi \neq R$ ist, folgt aus Proposition 2.6 dass $\ker \varphi = \{0\}$. Also ist φ injektiv (Bemerkung 1.7). □

Definition 2.8.
$M \lhd R$ ist *maximal*, wenn

(i) $M \neq R$ (M ist echt).

(ii) Ist $I \lhd R$ mit $M \subseteq I \subseteq R$,

dann gilt: $I = M$ oder $I = R$ (i.e. es gibt keine weiteren Ideale strikt zwischen M und R).

Proposition 2.9.
Jedes echte Ideal ist in einem Maximalideal enthalten.

Um Proposition 2.9 zu beweisen, brauchen wir Zorn's Lemma.

Exkurs

Partielle Ordnung
Sei $A \neq \varnothing$ eine Menge. Eine *partielle Ordnung* auf A ist eine Relation $\leq$ auf A mit den Eigenschaften:

(1) $x \leq x$ für alle $x \in A$.

(2) Aus $x \leq y$ und $y \leq x$ folgt $x = y$ für alle $x, y \in A$.

(3) Aus $x \leq y$ und $y \leq z$ folgt $x \leq z$ für alle $x, y, z, \in A$.

(4) $\leq$ ist *total* falls $x \leq y$ oder $y \leq x$ für alle $x, y \in A$.

Definition

(i) Sei $(A, \leq)$ eine partielle Ordnung und $B \subseteq A$. Ein Element $a \in A$ heißt *obere Schranke* für B in A, falls $b \leq a$ für alle $b \in B$.

(ii) $m \in A$ heißt *maximal*, wenn gilt: $m \leq x \Rightarrow m = x$ für alle $x \in A$.

Zorn's Lemma
Sei $A \neq \varnothing$ eine partielle Ordnung mit der Eigenschaft: Jede total angeordnete Teilmenge $B \subseteq A$ hat eine obere Schranke in A. Dann hat A ein maximales Element.

Ende Exkurs.

Beweis von Proposition 2.9:
Sei $I \lhd R$, $I \subsetneq R$. Betrachte
$S :=$ die Menge aller echten Ideale von R, die I enthalten.
$I \in S$, so $S \neq \varnothing$.
S ist partiell geordnet durch Mengeninklusion. Wir behaupten, dass jede total geordnete Teilmenge von S eine obere Schranke in S hat. Sei also $\xi \subseteq S$ eine solche. Setze

$$J := \bigcup_{c \in \xi} C$$

J ist Ideal: $0 \in J$. Seien $a, b \in J$, existieren $C_1, C_2 \in \xi$ mit $a \in C_1$ und $b \in C_2$.
Nun gilt $C_1 \subseteq C_2$ oder $C_2 \subseteq C_1$ (weil ξ total geordnet ist).
In jedem Fall ist $a + b \in J$ (weil $a + b \in C_1$ oder $a + b \in C_2$).
Analog zeigt man: $a \in J$ und $r \in R \Rightarrow ra \in J$.
Nun zeigen wir: $J \subsetneq R$, sonst $1 \in J$, also $1 \in C$ für ein geeignetes $C \in \xi$ - Widerspruch, weil $C \in \xi$ echt sein muss.

Anwendung von Zorn's Lemma ergibt:
S hat maximale Elmente. Wenn M ein solches ist, dann ist klar, dass M ein maximales Ideal ist, welches I enthält, wie behauptet. □

3 Script zur Vorlesung: Algebra 1 (WiSe2020-2021)

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir Primideale und Maximalideale näher untersuchen. Danach werden wir Produktringe einführen. In diesem Zusammenhang werden wir den Chinesischer Reste-Satz aussagen und beweisen. Damit wird § 2 beendet. In § 3 führen wir Bruchringe ein.

Proposition 3.1.
$M \lhd R$ ist maximal genau dann, wenn R/M ein Körper ist.

Beweis:
M ist maximal, genau dann, wenn $M \subsetneq R$ und es keine Ideale A gibt mit

$$M \subsetneq A \subsetneq R$$

d.h. genau dann, wenn R/M nur $M/M = \{0\}$ und R/M als Ideale hat. Nun Proposition 2.6(2) anwenden. □

Beispiel 3.2.
$n\mathbb{Z} \lhd \mathbb{Z}$ ist maximal genau dann, wenn $\mathbb{Z}/n\mathbb{Z} \backsimeq \mathbb{Z}_n$ ein Körper ist, genau dann, wenn $n = p$ eine Primzahl ist (Lineare Algebra I, 3. Vorlesung).

Definition 3.3.
$P \lhd R$ ist ein Primideal, wenn

(1) P echt ist, i.e. $P \subsetneq R$.

(2) Für alle $a, b, \in R$: Aus $ab \in P$ folgt $a \in P$ oder $b \in P$.

Beispiel 3.4.
$\{0\} \neq p\mathbb{Z} \lhd \mathbb{Z}$ ist Primideal genau dann, wenn p eine Primzahl ist.

Proposition 3.5.
$P \lhd R$ ist Primideal genau dann, wenn R/P ein Integritätsbereich ist.

Beweis:
Per Definition von R/P gilt für $a, b \in R : \overline{ab} = \overline{a}\overline{b}$, und $\overline{a} = \overline{0}$ genau dann, wenn $a \in P$. Dies bedeutet wiederum: P Primideal genau dann, wenn $[\overline{ab} = \overline{a}\overline{b} = \overline{0} \Rightarrow \overline{a} = \overline{0}$ **oder** $\overline{b} = \overline{0}]$ genau dann, wenn R/P integer ist. □

Aus Proposition 3.1 und 3.5 folgt nun:

Korollar 3.6.
Jedes maximale Ideal ist Primideal.

Definition 3.7.

(1) Seien R, S Ringe. Wir definieren Ringoperationen auf $R \times S$ (koordinatenweise).

$$\left.\begin{array}{rcrcl} (r_1, s_1) & + & (r_2, s_2) & := & (r_1 + r_2, s_1 + s_2) \\ (r_1, s_1) & \times & (r_2, s_2) & := & (r_1 r_2, s_1 s_2) \end{array}\right\} \text{ für alle } r_1, r_2 \in R \text{ und } s_1, s_2 \in S$$

$R \times S$ heißt *Ringprodukt*.

(2) Seien $A, B \lhd R$, setze: $A + B := \{a + b; a \in A, b \in B\}$. A, B sind *teilerfremd*, wenn $A + B = R$

Konvention: In der Bezeichnung $\overline{x}$ für ein Element aus R/I, werden wir zur Erleichterung der Notation das Symbol $\bar{}$ unterbinden, wann immer der Kontext klar ist.

Satz 3.8. (Chinesischer Reste-Satz)
Seien R ein kommutativer Ring mit 1 und $A_1, \ldots, A_k \lhd R$. Die Abbildung

$$\begin{array}{rccc} \varphi: & R & \to & \prod_{i=1}^{k} (R/A_i) \\ & r & \mapsto & (r + A_1, \ldots, r + A_k) \end{array}$$

ist ein Ringhomomorphismus mit $\ker \varphi = \bigcap_{i=1}^{k} A_i$.

Wenn A_i, A_j teilerfremd sind für alle $i \neq j$, dann ist φ surjektiv. In diesem Fall gilt also:

$$R/\bigcap_{i=1}^{k} A_i \simeq \prod_{i=1}^{k} (R/A_i).$$

Beweis:

Ohne Einschränkung $k = 2$ (ÜA). Prüfe, für $r_1, r_2 \in R$ ob $\varphi(r_1 + r_2) \stackrel{?}{=} \varphi(r_1) + \varphi(r_2)$. Wir berechnen:

$$\begin{array}{rcl} \varphi(r_1 + r_2) & = & ((r_1 + r_2) + A_1, (r_1 + r_2) + A_2) \\ & = & ((r_1 + A_1) + (r_2 + A_1), (r_1 + A_2) + (r_2 + A_2)) \\ & = & (r_1 + A_1, r_1 + A_2) + (r_2 + A_1, r_2 + A_2) \\ & = & \varphi(r_1) + \varphi(r_2)\,. \end{array}$$

Analog berechnet man $\varphi(r_1 r_2)$ (ÜA). Also ist φ ein Ringhomomorphismus. Wir berechnen:

$$\begin{array}{rcl} \ker \varphi & = & \{r \in R\,;\, \varphi(r) = 0\} \\ & = & \{r \in R\,;\, \varphi(r) = (A_1, A_2)\} \\ & = & \{r \in R\,;\, r \in A_1 \text{ und } r \in A_2\}. \end{array}$$

Sei nun $A_1 + A_2 = R$. Es existieren also $x \in A_1$ und $y \in A_2$ mit $x + y = 1$.
Es folgt: $x - 1 \in A_2$ und $y - 1 \in A_1$, und somit $\varphi(x) = (0, 1)$ und $\varphi(y) = (1, 0)$.

Sei nun $(r_1 + A_1, r_2 + A_2) \in R/A_1 \times R/A_2$ beliebig. Setze $r := r_2 x + r_1 y$ und berechne:

$$\begin{array}{rcl} \varphi(r) & = & \varphi(r_2 x + r_1 y) \\ & = & \varphi(r_2)\varphi(x) + \varphi(r_1)\varphi(y) \\ & = & (r_2 + A_1, r_2 + A_2)(0, 1) + (r_1 + A_1, r_1 + A_2)(1, 0) \\ & = & (0, r_2 + A_2) + (r_1 + A_1, 0) \\ & = & (r_1 + A_1, r_2 + A_2). \end{array}$$

Also ist φ surjektiv.
Die letzte Aussage folgt aus Isomorphiesatz. □

§ 3 Bruchringe

Definition 3.9.
Seien R ein kommutativer Ring mit 1 und $D \subseteq R$. D ist multiplikativ, falls $1 \in D$ und $st \in D$ für alle $s, t \in D$.

Beispiel 3.10.

(i) $D = R^\times$

(ii) $D = R \backslash P$ mit $P \lhd R$ Prim.

Konstruktion:
Sei $D \subset R$ eine multiplikative Untermenge, ohne Nullteiler, und so dass $0 \notin D$. (*)

Definiere eine Relation $\sim$ auf $R \times D$:

$$(r, d) \sim (r', d') \Leftrightarrow rd' = dr' .$$

$\sim$ ist Äquivalenzrelation, wir zeigen z.B. die Transitivität:

$$\begin{array}{rccc|c|rcccl} & (r,d) & \sim & (s,e) & \Rightarrow + & re & - & sd & = 0 & \times f \\ \text{und} & (s,e) & \sim & (t,f) & & sf & - & te & = 0 & \times d \end{array} \quad \text{ergibt } (rf - td)e = 0,$$

Außerdem ist e ist kein Nullteiler und $e \neq 0$. Also muss $rf - td = 0$ sein und damit $rf = td$. Also $(r, d) \sim (t, f)$.

Notation:
Schreibe $\frac{r}{d} := [(r, d)]$ (die Äquivalenzklasse von (r, d)) und setze $D^{-1}R :=$ die Menge der Äquivalenzklassen.

Wir Versehen $D^{-1}R$ mit den folgenden Verknüpfungen:

$$\frac{r_1}{d_1} + \frac{r_2}{d_2} := \frac{r_1 d_2 + r_2 d_1}{d_1 d_2} \quad \text{und} \quad \frac{r_1}{d_1} \cdot \frac{r_2}{d_2} := \frac{r_1 r_2}{d_1 d_2}.$$

Im Skript 4 werden wir zeigen dass $D^{-1}R$ ein Ring ist, und werden seine Eigenschaften weiter untersuchen.

4 Script zur Vorlesung: Algebra 1 (WiSe2020-2021)

Prof. Dr. Salma Kuhlmann

In diesem Skript beweisen wir (wie angekündigt am Ende vom Skript 3) Satz 4.2, und liefern wichtige Beispiele. Im Abschnitt 4 untersuchen wir Polynomringe über Ringe; siehe Satz 4.8. Wir beenden mit dem wichtigem Besipiel 4.11.

Definition 4.1. Ein injektiver Ringhomomorphismus heißt eine *Einbettung*.

Ansatz:
R kommutativer Ring mit 1, $D \subset R$ multiplikative Untermenge ohne Nullteiler, $0 \notin D$. (*)

Satz 4.2.
$D^{-1}R$ ist ein kommutativer Ring mit Eins. Die Abbildung

$$\begin{array}{rccc} i: & R & \to & D^{-1}R \\ & r & \mapsto & \frac{r}{1} \end{array}$$

definiert eine Einbettung mit $i(D) \subseteq (D^{-1}R)^\times$.

Beweis:
Wir zeigen, dass die Addition wohldefiniert ist.

Seien also $\frac{a}{b} = \frac{a'}{b'}$, und $\frac{c}{d} = \frac{c'}{d'}$. Wir müssen zeigen dass: $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$.

Wir prüfen:

$$\begin{array}{ccc} \frac{a}{b} = \frac{a'}{b'} & \text{und} & \frac{c}{d} = \frac{c'}{d'} \\ \Downarrow & & \Downarrow \\ ab' = a'b & & cd' = c'd \\ (ad+bc)(b'd') & \stackrel{?}{=} & (a'd'+b'c')(bd) \\ \text{berechne} & & \text{und vergleiche} \\ \| & & \| \\ \underline{ab'}dd' + \underline{\underline{cd'}}bb' & = & \underline{a'b}dd' + \underline{\underline{c'd}}bb' \end{array}$$

Also gilt die Gleichung.

Analog zeigen Sie dass die Multiplikation wohldefiniert ist, dass die Ringaxiome für $D^{-1}R$ gelten, das Nullelement $\frac{0}{1}$ und Einselement $\frac{1}{1}$ sind (ÜA).

Prüfen Sie dass die Abbildung i ein Ringhomomorphismus ist (ÜA). Per Definition von i gilt: $i(r) = 0 \Leftrightarrow \frac{r}{1} = \frac{0}{1} \Leftrightarrow r = 0$. Also ist i injektiv.

Für $d \in D$ ist $i(d) = \frac{d}{1}$ und damit $i(d)^{-1} = \frac{1}{d}$. □

Konvention: Wir identifizieren R mit $i(R)$ (i.e. r mit $\frac{r}{1}$ für alle $r \in R$). Somit wird R mit dem Teilring $i(R)$ von $D^{-1}R$ identifiziert.

Definition 4.3.
$D^{-1}R$ ist der *Ring von Brüchen von R bezüglich D.*

Satz 4.4.
Jeder Integritätsbereich lässt sich in einen Körper einbetten.

Beweis:
Wenn R integer ist, dann erfüllt $D = R\backslash\{0\}$ die Bedingung $(*)$. Dann ist $D^{-1}R$ ein Körper (wenn $0 \neq \frac{r}{d}$ dann ist $r \neq 0$ und $(\frac{r}{d})^{-1} = \frac{d}{r}$). □

Notation: Wenn R integer ist und $D = R\backslash\{0\}$ bezeichnen wir den Körper $D^{-1}R$ mit **Quot (R)**.

Korollar 4.5.
Der Ring R läßt sich in einen Körper einbetten genau dann, wenn er integer ist.

Beispiel 4.6.
Quot $(\mathbb{Z}) = \mathbb{Q}$

Definition 4.7.
P ist ein Primideal; $D = R \setminus P$.
$R_P := D^{-1}R$ bezeichnet die *Lokalisierung von R nach P.*

§ 4 Polynomringe über Ringe

Erinnerung:
• $R[x] := \{p(x) \ ; \ p(x)$ Polynom über $R\}$

$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a, x + a_0$

$n \in \mathbb{N}_0 \left[\begin{array}{rcl} 0 \neq a_n & := & \text{Leitkoeffizient} \\ \deg p & := & n \end{array} \right.$

• $R \subseteq R[x]$ als Teilring der konstanten Polynome (i.e. Polynome p mit $\deg p = 0$).
• Addition: Koordinatenweise (koeffizientenweise)
• Multiplikation: wenn $p(x) = \sum a_i x^i$ und $q(x) = \sum b_j x^j$,
so ist der Koeffizient von x^k im Produkt $p(x)q(x)$ gleich $\sum_{i=0}^{k} a_i b_{k-i}$.
• Wir beantworten nun die Frage: Wann ist $a_n b_m$ Leitkoeffizient vom Produkt $p(x)q(x)$?
Siehe dazu den Beweis vom Satz 4.8.

Satz 4.8.
R ist integer genau dann, wenn $R[x]$ integer ist.

Beweis
"⇐" Ein Teilring von einem Integritätsbereich ist integer.

"⇒" Sei $a_n \neq 0$ und $b_m \neq 0$ für $p(x) = a_n x^n + \cdots + a_o$ und $q(x) = b_m x^m + \cdots + b_o$, dann ist $a_n b_m \neq 0$, weil R integer ist (und damit ist auch $\deg p(x)q(x) = n + m$). Insbesondere ist $p(x)q(x)$ nicht das Nullpolynom. □

Definition 4.9.
Sei K ein Körper. Dann ist Quot $(K[x]) := K(x)$ der *rationale Funtkionenkörper einer Variablen über K.*

Bemerkung 4.10.
Sei R ein Ring. Betrachte die Abbildung

$$\begin{array}{rccc} ev_0: & R[x] & \twoheadrightarrow & R \\ & p(x) & \mapsto & p(0) \quad = \quad \text{der konstante Term von } p(x). \end{array}$$

Dann ist ev_0 ein surjektiver Ringhomomorphismus (ÜA). Wir berechnen:

$$\ker ev_0 =< x >= \{xf(x); f(x) \in R[x]\}$$

(das Ideal der Polynome mit konstantem Term gleich Null).

Es folgt aus Isomorphiesatz dass $R[x]/ < x > \simeq R$.

Beispiel 4.11. Sei nun $R = \mathbb{Z}$, so ist $\mathbb{Z}[x]/ < x > \simeq \mathbb{Z}$.

Wir sehen also (siehe Proposition 3.1 und 3.5): $< x >$ ist ein Primideal in $\mathbb{Z}[x]$, aber ist nicht maximal.

5 Script zur Vorlesung: Algebra 1 (WiSe2020-2021)

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir einige Begriffe (die wir schon in der LA I für den Ring $\mathbb{Z}$ und in der LA II für den Ring $K[x]$ kennengelernt hatten) allgemeiner für kommutative Ringe einführen. Wir werden im Abschnitt 6 Ringe erhalten, die einen Divisionsalgorithmus und Euklidische Algorithmus (zum Berechnen von ggT) besitzen. Im Abschnitt 7 werden wir eine strikt größere Klasse studieren.

§ 5 Teilbarkeit

Sei R stets ein kommutativer Ring mit Eins.

Definition 5.1.
Seien $a, b \in R; b \neq 0$

(i) b *teilt* a, wenn ein $x \in R$ existiert mit $a = bx$. (Bezeichnung: $b|a$)

(ii) $d \in R$ ist ein *gemeinsamer Teiler von a und b* (Bezeichnung: gT von a, b) falls $d|a$ und $d|b$

(iii) $d \in R$ ist ein *ggT von a und b*, falls

(a) d ist ein gT von a und b, und für alle $d' \in R$ gilt:

(b) $d'|a$ und $d'|b$ impliziert $d'|d$.

Bemerkung 5.2.

(i) $b|a$ genau dann, wenn $a \in < b >$ (genau dann, wenn $< a > \subseteq < b >$)

(ii) d ist gT von a, b genau dann, wenn $< a, b > \subseteq < d >$

(iii) d ist ggT von a, b genau dann, wenn d ist gT von a, b und für alle $d' \in R$ gilt: $< a, b > \subseteq < d' >$ impliziert $< d > \subseteq < d' >$.

Aus Bemerkung 5.2 bekommen wir eine hinreichende Bedingung für die $\exists^Z$ eines ggT:

Proposition 5.3.

Seien $a, b \in R$ so dass $< a, b >$ ein Hauptideal ist, i.e. $< a, b > = < d >$, dann ist d ein ggT von a und b.

Die Bedingung ist jedoch nicht notwendig, siehe ÜB.

Definition 5.4.
$x, y \in R$ sind *assoziiert*, falls ein $u \in R^\times$ exisitert mit $xu = y$.

Proposition 5.5. (Eindeutigkeit bis auf Einheiten)

Sei R integer, $d, d' \in R$ und $a, b \in R$.
Es gilt: $< d > = < d' >$ genau dann, wenn d, d' assoziiert sind.
Insbesondere alle ggT von a, b sind zueinander assoziiert.

Beweis:

"$\Leftarrow$" $d' = ud \Leftrightarrow d = d'u^{-1}$ mit $u \in R^\times$. Also $d' = ud \Rightarrow d' \in < d > \Rightarrow < d' > \subseteq < d >$ und umgekehrt aus $d = d'u^{-1}$ folgt auch $< d > \subseteq < d' >$.

"$\Rightarrow$" Seien $d, d' \neq 0$ und $< d > = < d' >$. Also

$$\left.\begin{array}{ll} \exists x \in R & : \ d = xd' \\ \exists y \in R & : \ d' = yd \end{array}\right\| \Rightarrow d = xyd \text{ i.e. } d(1 - xy) = 0$$

R integer und $d \neq 0$ impliziert $1 - xy = 0$, also $xy = 1$.

Die letzte Aussage folgt aus Bemerkung 5.2. □

§ 6 Euklidische Bereiche

Definition 5.6.

(1) Eine Abbildung $N : R \setminus \{0\} \to \mathbb{N}_0$ heißt *Norm.*

(2) Der Integritätsbereich R, versehen mit der Norm N, heißt *euklidisch* (R ist E.R.), wenn er einen Divisionsalgorithmus bezüglich N erlaubt, das heißt:
für $\forall a, b \in R$ mit $b \neq 0$ $\exists q, r \in R$, so dass $a = qb + r$, wobei $r = 0$ oder $N(r) < N(b)$.

Beispiel 5.7.

(i) $\mathbb{Z}$ mit $N(a) := |a|$

(ii) $K[x]$, wenn K *ein Körper* mit $N(p(x)) := \deg p(x)$ ist.

Weitere Beispiele: Siehe ÜB.

Proposition 5.8.
Sei R ein euklidischer Integritätsbereich, $I \lhd R$, dann ist I ein Hauptideal.

Beweis:
Sei $I \neq \{0\}$ und $0 \neq d \in I$, also $< d > \subseteq I$. Wähle d so dass $N(d)$ minimal ist. Sei nun $a \in I$ und $q, r \in R$ mit $a = qd + r$ wobei $r = 0$ oder $N(r) < N(d)$. Da $r = a - qd \in I$, ist $N(r) < N(d)$ nicht möglich. Also $r = 0$ und somit $a = qd \in < d >$. □

Eine wichtige Eigenschaft von E.R. ist die $\exists^Z$ eines ggT sowie eines Algorithmus zum Berechnen von ggT . Die Aussage und Beweis vom Satz 5.9 haben wir im LA I (Rückwärts EA; Skript 3 Seiten 2 und 3) für $R = \mathbb{Z}$ (und in LA II Skripte 3 und 5 für $R = K[x]$) detailliert studiert. Wir wiederholen hier die Beweisschritte nicht ausführlich.

Satz 5.9.
Sei R E.R; $a, b \in R \neq 0$ und $d = r_n$ der letzte ungleich Null Rest in **(DA)**. Dann ist

(1) d ein ggT von a und b

(2) $d = ax + by$ für geeignete $x, y \in R$.

Beweis: Wiederholter Anwendung des Divisionsalgorithmus (DA)
Seien $a, b \in R, b \neq 0$

$$\begin{array}{lllll} a & = & q_0 b & + & r_0 \\ b & = & q_1 r_0 & + & r_1 \\ r_0 & = & q_2 r_1 & + & r_2 \\ \vdots & & & & \\ r_{n-2} & = & q_n r_{n-1} & + & r_n \quad r_n \neq 0 \\ r_{n-1} & = & q_{n+1} r_n & & (*) \end{array}$$

(Da

$$N(b) > N(r_0) > \cdots > N(r_{n-1}) > N(r_n) \geq 0$$

kann der Abstieg nur endlich viele Schritte n haben, das Verfahren muss also zwangläufig mit einer Gleichung $(*)$ anhalten). □

§ 7 Hauptidealbereiche

Definition 5.10.
Ein *Hauptidealbereich* (H.I.R.) ist ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist.

Proposition 5.11.
Sei R ein Hauptidealbereich, $a, b \neq 0, a, b \in R$ und d ein Erzeuger von $< a, b >$. Es gelten:

(1) d ist ggT von a, b

(2) $\exists x, y \in R$ mit $d = ax + by$

(3) d ist (bis auf Einheiten) eindeutig.

Beweis:
Folgt aus Proposition 5.2, Bemerkung 2.3 (3) und Proposition 5.5. □

Proposition 5.12.
Jedes Primideal in einem Hauptidealbereich ist auch maximal.

Beweis:
Sei $< p > \neq \{0\}$ Primideal und $M \supseteq < p >, M$ maximal (M existiert vgl. Proposition 2.9).
Nun ist auch $M = < m >$ ein Hauptideal und $p \in < m >$. Also existiert $r \in R$ mit $p = rm$.
Aber $< p >$ prim $\Rightarrow r \in < p >$ oder $m \in < p >$.
1. Fall: $m \in < p > \Rightarrow < m > \subseteq < p > \Rightarrow < p > = M$
2. Fall: $r \in < p > \Rightarrow r = ps \Rightarrow p = psm$, kürzen ergibt: $sm = 1$. Somit ist aber $m \in R^\times$. Das widerspricht, dass M maximal, also echt, ist (vgl. Proposition 2.6(1)). □

Beispiel 5.13.

(1) Alle Ideale in $\mathbb{Z}$ sind Hauptideale der Gestalt $n\mathbb{Z}$, $n\mathbb{Z}$ ist maximal genau dann, wenn $n = p$ eine Primzahl ist.

(2) $\mathbb{Z}[x]$ ist kein Hauptidealbereich, weil $< x >$ prim, aber nicht maximal ist (Beispiel 4.11).

Wir verallgemeinern Beispiel 5.13 (2):

Korollar 5.14.
Sei R integer, $R[x]$ ist ein Hauptidealbereich genau dann, wenn R ein Körper ist.

Beweis:
"$\Leftarrow$" R ist ein Körper $\Rightarrow R[x]$ ist E.R. (s. Beispiel 5.7 (ii)) $\Rightarrow R[x]$ ist H.I.R. (s. Prop. 5.8).

"$\Rightarrow$" $R[x]/ < x > \simeq R$ (vgl. Bemerkung 4.10), also ist $< x >$ Primideal (s. Proposition 3.5).

Nun $R[x]$ Hauptidealbereich $\Rightarrow < x >$ ist ein maximales Ideal (s. Proposition 5.12) $\Rightarrow R[x]/ < x >$ ist ein Körper (s. Proposition 3.1) . □

6 Script zur Vorlesung: Algebra 1 (WiSe2020-2021)

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir zunächst prime und irreduzible Elemente in einem integer Ring einführen und studieren. Im Abschnitt 9 werden wir dann unsere Untersuchung über Faktorielle Ringe beginnen.

§ 8 Primelemente, Irreduzible Elemente

Sei R stets ein integer Ring.

Definition 6.1.

(1) Sei $0 \neq p \in R$, p ist *Primelement*, wenn $< p >$ *Primideal* in R ist
(für alle $a, b \in R : p|ab \Rightarrow p|a$ oder $p|b$).

(2) Sei $0 \neq r \in R$; $r \notin R^\times$, p ist *irreduzible* in R, wenn für alle $a, b \in R : r = ab \Rightarrow a \in R^\times$ oder $b \in R^\times$. Sonst ist r *reduzible*.

Proposition 6.2.
Sei $p \in R$, p ist Primelement $\Rightarrow p$ ist irreduzible.

Beweis:
Sei $< p > \neq \{0\}$ Primideal. Also ist $p \notin R^\times$.
Wenn $p = ab$ dann folgt: $ab \in < p > \Rightarrow a \in < p >$ oder $b \in < p >$.
1. Fall: $a \in < p > \Rightarrow a = pr \Rightarrow p = prb$ oder $p(1 - rb) = 0 \Rightarrow 1 = rb$; also $b \in R^\times$.
2. Fall: Analog. □

Proposition 6.3.
Sei R Hauptidealbereich, $p \in R$ irreduzible $\Rightarrow p$ ist Primelement.

Beweis:
Sei $p \notin R^\times; p \neq 0$, p irreduzible.
Sei $M \lhd R$ ein Ideal so dass $< p > \subseteq M$. Nun existiert ein $m \in R$ mit $M = < m >$.
Also $\exists r : p = rm$ und p irreduzible, also

1. Fall		2. Fall
$r \in R^\times$	oder	$m \in R^\times$
$\Downarrow$		$\Downarrow$
$< p >=< m >$		$< m >= R$

Wir haben gezeigt dass $< p >$ maximal, und insbesondere Primideal ist. □

§ 9 Faktorielle Ringe

Definition 6.4.
R ist *faktoriell*, wenn

(1) Für alle $0 \neq r \in R \setminus R^\times$ existiert $p_1, \ldots, p_n \in R$ irreduzibel: $r = p_1 \cdots p_n$ (†)

(2) Diese Darstellung ist *eindeutig bis auf die Reihenfolge und Assoziiertheit*:
D.h. wenn auch $r = q_1 \cdots q_m$ mit $q_1, \ldots, q_m$ irreduzible, dann ist $m = n$
und $\forall$ i $\exists$ j und $u_i \in R^\times$ so dass: $u_i p_i = q_j$.

(3) Also R ist faktoriell wenn für jedes $r \in R$, $r \neq 0$ beliebiges Element, gibt es für r eine Darstellung

$$r = u p_1^{e_1} \cdots p_n^{e_n}$$

mit $u \in R^\times, e_i \in \mathbb{N}_0$, p_i irreduzible, mit $p_i \neq p_j$ für $i \neq j$. (†)

Für faktorielle Ringe gilt auch die Umkehraussage von Proposition 6.2:

Proposition 6.5.
Sei R faktoriell und $p \in R$, es gilt: p irreduzible $\Rightarrow p$ ist Primelement.

Beweis:
Sei $0 \neq p$, $p \in R \setminus R^\times$ irreduzible und $a, b \in R$ mit $p|ab$. Nun $p|ab \Rightarrow ab = pc$ für ein $c \in R$ $(*)$
Schreibe a und b wie in (†).
Da p irreduzibel ist, folgt aus $(*)$ und der Eindeutigkeit in (†): p ist assoziiert mit einem der irreduziblen Faktoren in der Darstellung von a oder von b.
Ohne Einschränkung sei es a, und schreibe $a = (up)p_2 \cdots p_n$; $u \in R^\times$, $p_i \in R$. Somit haben wir bewiesen dass $p|a$. □

Auch für faktorielle Ringe gilt die Existenz eines $ggTs$ (vgl. Satz 5.9):

Proposition 6.6.
Sei R faktoriell, a und $b \in R$. Schreibe:
$a = u p_1^{e_1} \cdots p_n^{e_n}$ (†)
$b = v p_1^{f_1} \cdots p_n^{f_n}$ (‡)

wobei $u, v \in R^\times$, p_i irreduzible, $p_i \neq p_j$ für $i \neq j$, e_i , $f_i \in \mathbb{N}_0$.

Setze $d := p_1^{min(e_1, f_1)} \cdots p_n^{min(e_n, f_n)}$ (††)
Dann ist d ein ggT von a und b.

Beweis:
Aus (††), (‡) und (†) ist klar, dass $d|a$ und $d|b$. Sei $d' \in R$ so dass, $d'|a$ und $d'|b$. Schreibe in der (†) Darstellung, mit q_i irreduzibel:

$$d' = v q_1^{g_1} \cdots q_n^{g_n} .$$

Nun für alle i : $q_i|d' \Rightarrow q_i|a$ und $q_i|b$.
Also für alle i : $q_i|a \Rightarrow$ existiert ein j und $u_i \in R^\times$ so dass $p_j = u_i q_i$.
Also $g_\ell \leq e_\ell$. Analog zeigt man dass $g_\ell \leq f_\ell$. Also $g_\ell \leq min(e_\ell, f_\ell)$. Somit haben wir gezeigt: $d'|d$. □

Satz 6.7.
Sei R ein Hauptidealbereich, dann is R faktoriell.

Beweis:
Sei $0 \neq r \in R \setminus R^\times$. Wir wollen eine Darstellung (†) erreichen.
Ist r irreduzibel, dann ist das Ziel erreicht. Sonst zerlege $r = r_1 r_2$, $r_1 \notin R^\times$ und $r_2 \notin R^\times$.
Sind r_1, r_2 irreduzibel, dann ist das Ziel erreicht. Sonst zerlege $r_1 = r_{11} r_{12}$, usw.

Diese Prozedur muss nach endlich vielen Schritten anhalten, da wir sonst eine unendliche (**strikte**) für die Inklusion ansteigende Folge von Idealen bekommen:

$$< r > \subsetneq < r_1 > \subsetneq < r_{11} > \subsetneq \cdots \subseteq R\,.$$

Wir behaupten nun, dass dieses in einem Hauptidealbereich nicht der Fall sein kann:

Sei also $I_i \lhd R$ mit $I_1 \subseteq I_2 \subseteq \cdots \subseteq R$.
Setze $I := \bigcup_{i=1}^{\infty} I_i \lhd R$. Da R ein Hauptidealbereich, existiert $a \in R$ mit $I = < a >$.
Nun $a \in I \Rightarrow \exists n \in \mathbb{N} : a \in I_n$. Also $I_n \subseteq I = < a > \subseteq I_n$ und somit $I = I_n$.
Damit ist die Behauptung bewiesen.

Wir haben also die $\exists^Z$ einer Darstellung (†) gezeigt. Die Aussage über die Eindeutigkeit erfolgt per Induktion über n in der Darstellung $r = p_1 \cdots p_n$ (genau so wie in Lineare Algebra II, Skript 5 Seite 3, Beweis vom Satz 5.15). □

7 Script zur Vorlesung: Algebra 1 (WiSe2020-2021)

Prof. Dr. Salma Kuhlmann

Bisher haben wir zwei Hauptthemen untersucht: Wir haben einerseits diese Inklusionen Körper ⊆ Euklidische Bereiche ⊆ Hauptidealbereiche ⊆ Faktorielle Bereiche ⊆ Integritätsbereiche untersucht und andererseits haben wir Polynomringe über Integerringe untersucht. In diesem Skript werden wir diese zweite Untersuchung fortsetzen. Unser Ziel ist es, Satz 4.8 ähnlich für faktorielle Ringe zu zeigen.

§ 10 Polynomringe über faktorielle Ringe

Sei R stets integer.

Lemma 7.1.
$R[x]$ ist faktoriell $\Rightarrow R$ ist faktoriell.

Beweis:
Da R integer ist, wissen wir dass $\deg p(x)q(x) = \deg p(x) + \deg q(x)$ für alle $0 \neq p, q \in R[x]$ $(*)$ (und dass auch $R[x]$ integer ist; siehe Satz 4.8 und seinen Beweis). Aus $(*)$ folgt dass $(R[x])^\times = R^\times$ und $r \in R$ ist irreduzibel in $R[x]$ genau dann, wenn r irreduzibel in R ist. $(**)$ (ÜA).
Sei nun $0 \neq r \in R \setminus R^\times$, per Annahme ist r das Produkt vom Irreduziblen in $R[x]$ (und diese Darstellung ist eindeutig bis auf Reihenfolge und Assoziiertheit). Diese irreduzible Faktoren müssen wegen $(*)$ Grad 0 haben, d.h. die Faktoren sind Elemente aus R. Wegen $(**)$ sind diese Faktoren irreduzible auch in R. Wir haben eine Darstellung wie in Definition 6.4(1) (†) bekommen. Die Eindeutigkeit Bedingung in Definition 6.4(2) wird analog geprüft. □

Um die Umkehrung von Lemma 7.1 zu etablieren (siehe Skript 8) brauchen wir hier das Lemma von Gauß. Hierfür brauchen wir wiederum das Hilfslemma 7.2:

Lemma 7.2.
Sei $I \lhd R$. Dann gelten für das Ideal $< I > \lhd R[x]$:

1. $< I >= I[x] := \{f(x) \in R[x]\,;\ \ f(x) = \sum a_i x^i \text{ mit } a_i \in I\}$
2. $R[x]/I[x] \simeq (R/I)[x]$
3. I ist Primideal in $R \Rightarrow I[x]$ ist Primideal in $R[x]$.

Beweis:
Die 1. Aussage ist leicht zu prüfen. Betrachte nun $\begin{array}{rccc} \varphi: & R[x] & \to & (R/I)[x] \\ & \sum a_i x^i & \mapsto & \sum \overline{a_i} x^i \end{array}$

Es ist leicht zu prüfen dass φ ein Ringhomomorphismus ist; dass φ surjektiv ist; und dass $\ker \varphi = I[x]$. Die 2. und 3. folgen nun aus Isomorphiesatz sowie Proposition 3.5 und Satz 4.8. □

Lemma 7.3. (Lemma von Gauß)
Sei R faktoriell, $F := \text{Quot}(R)$ und $p(x) \in R[x]$. Wenn $p(x)$ reduzibel in $F[x]$ ist, so ist $p(x)$ reduzibel in $R[x]$. Genauer: Wenn

$$p(x) = A(x)B(x), A, B \in F[x], \deg A \geq 1, \deg B \geq 1\,,$$

dann gibt es $0 \neq r, 0 \neq s \in F$ so dass

$$\left.\begin{array}{l} rA(x) := a(x) \\ sB(x) := b(x) \end{array}\right\} \in R[x] \qquad \deg a(x) \geq 1, \deg b(x) \geq 1$$

und $p(x) = a(x)b(x) \in R[x]$.

Beweis:

$$\begin{array}{ccccc} p(x) & = & A(x) & & B(x) \\ \uparrow & & \uparrow & & \uparrow \\ R[X] & & F[x] & & F[x] \end{array}$$

Die Koeffizienten von A, B sind aus der Form $\frac{r_i}{s_i}$ mit $r_i, 0 \neq s_i \in R$. Wir multiplizieren A, B jeweils mit den gemeinsamen Nennern seiner Koeffizienten und bekommen eine Gleichung:

$$\left.\begin{array}{ccccc} dp(x) & = & a'(x) & & b'(x) \\ \uparrow & & \uparrow & & \uparrow \\ d \in R & & \in R[x] & & \in R[x] \end{array}\right\} \text{ mit } d \in R, d \neq 0; \deg a'(x) \geq 1, \deg b'(x) \geq 1; a', b' \in R[x]. \qquad (*)$$

und $a'(x) = \alpha A(x), b'(x) = \beta B(x); \alpha, \beta \in F$.

1. Fall: $d \in R^\times$ ✓ (die Behauptung gilt in diesem Fall).

2. Fall: $d \in R \setminus R^\times$
So schreibe $d = p_1 \cdots p_n$, mit p_i irreduzibel in R für alle i.

- p_1 irreduzibel in $R \Rightarrow I :=< p_1 >$ ist Primideal in R und $d \in I$.
- $I[x] = p_1 R[x]$ Primideal in $R[x]$, $R[x]/I[x] \simeq (R/I)[x]$ und $(R/I)[x]$ ist integer (vgl. Lemma 7.2).

Wir reduzieren die Gleichung (*) mod I. Wir bekommen $0 = \overline{a'(x)b'(x)}$ in $(R/I)[x]$. Also ist ohne Einschränkung $\overline{a'(x)} = 0$, das heißt alle Koeffizienten von $a'(x)$ liegen in I sind also durch p_1 teilbar in R. So hat man $a''(x) := \frac{1}{p_1}a'(x) \in R[x], \deg a''(x) \geq 1$ mit $\frac{1}{p_1} \in F$, das heißt wir können die Gleichung (*) um p_1 kürzen und bekommen eine neue Gleichung

$$d'p(x) = a''(x)b''(x) \text{ in } R[x].$$

Aber nun hat d' einen irreduziblen Faktor weniger, i.e. $d' = p_2 \cdots p_n$.

Wiederholung mit $p_2, \ldots, p_n$ (gleiche Argumente) ergibt eine Gleichung schließlich aus der Form

$$\begin{array}{lccll} & p(x) & = & a(x)b(x) & a(x), b(x) \in R[x] \\ \text{mit} & a(x) & = & \alpha' a'(x) & \alpha', \beta' \neq 0 \\ & b(x) & = & \beta' b'(x) & \alpha', \beta' \in F \end{array}$$

$$\text{d.h.} \quad \begin{array}{ccc} a(x) & = & \alpha\alpha' A(x) \\ b(x) & = & \beta\beta' B(x) \end{array} \quad \text{mit } \alpha\alpha' \in F \text{ und } \beta\beta' \in F. \qquad \square$$

Korollar 7.4.
Sei R faktoriell, $F := \text{Quot}\,(R); \deg p \geq 1$, wobei $\sum_{i=0}^{n} a_i x^i =: p(x) \in R[x]$
mit ggT von $\{a_0, \ldots, a_n\} = 1$.
Dann ist $p(x)$ in $R[x]$ irreduzibel genau dann, wenn $p(x)$ in $F[x]$ irreduzibel. Insbesondere ist $p(x) \in R[x]$ normiert und in $R[x]$ irreduzibel, so ist $p(x)$ in $F[x]$ irreduzibel.

Beweis:
GL ergibt: Ist $p(x)$ in $F[x]$ reduzibel, so ist $p(x)$ in $R[x]$ reduzibel. Umgekehrt ist $p(x)$ in $R[x]$ reduzibel, dann ist $p(x) = a(x)b(x)$, wobei $a(x), b(x) \in R[x] \setminus R$ (sonst wäre der ggT der Koeffizient von $p(x)$ in R ungleich 1).
Das heißt $p(x) = a(x)b(x)$ für $a(x), b(x) \in R[x], \deg a(x) \geq 1, \deg b(x) \geq 1$. Insbesondere $p(x) = a(x)b(x)$ für $a(x), b(x) \in F[x], \deg a(x) \geq 1, \deg b(x) \geq 1$, das heißt $p(x)$ ist in $F[x]$ reduzibel. □

Wie angekündigt werden wir im Skript 8 die Umkehrung von Lemma 7.1 zeigen; wir werden wir zeigen dass R faktoriell impliziert $R[x]$ faktoriell. Eigentlich werden wir das Resultat auch für $R[x_1, \ldots, x_n]$ erhalten. Wir beenden Skript 7 mit einem Exkurs. Hier führen wir diesen Ring ein, und fassen einige Begriffe zusammen.

Exkurs $R[x_1, \ldots, x_n] := R[x_1, x_2, \ldots, x_{n-1}][x_n]$.
Notation $= \{p(x_1, \ldots, x_n) | p \in R[x_1, \ldots, x_n]\}$.

Also: *Polynome* in den Variablen $x_1, \ldots, x_n$ werden folgendermaßen definiert:
Es ist eine endliche Sumem von *Monomen*.

$$m(x_1, \ldots, x_n) := a x_1^{d_1} \cdots x_n^{d_n} \qquad a \in R$$

$$\text{Notation} \quad \begin{cases} := a \underline{x}^{\underline{d}} & d_i \in \mathbb{N}_0 \\ (x_1, \ldots, x_n) := \underline{x} \\ (d_1, \ldots, d_n) := \underline{d} \in \mathbb{N}_0^n \end{cases}$$

- d_i ist der *Grad von* x_i in $m(\underline{x})$
- $|\underline{d}| := \sum_{i=1}^{n} d_i$ ist der *Grad von* $m(\underline{x})$ $\deg m(\underline{x}) := |\underline{d}|$
- $\deg p(x_1, \ldots, x_n)$ ist der größte Grad von seinen Monomen.
- Die Summe aller Monomen von $p(x_1, \ldots, x_n)$ vom Grad k heißt die *homogene Komponente von p vom Grad k*.
- Wenn $\deg p = d$, so läßt sich p eindeutig als Summe

$$p = p_0 + p_1 + \cdots + p_d$$

beschreiben, wobei p_k die homogene Komponente vom Grad k ist für $0 \leq k \leq d$ (und $p_k = 0$ vorkommen kann).

8 Script zur Vorlesung: Algebra 1 (WiSe2020-2021)

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir den im Skript 7 angekündigten Beweis von Satz 8.1 führen. Der letzte Abschnitt 11 im Kapitel 1 wird für Irreduzibilitätsteste und Beispiele gewidmet. Damit beenden wir Kapitel 1.

Sei hier R stets ein integer Ring.

Satz 8.1.
R ist genau dann faktoriell wenn $R[x]$ faktoriell ist.

Beweis:
Die Rückrichtung ist Lemma 7.1 und wurde bereits gezeigt.
Sei R faktoriell. Seien $F = \text{Quot}\,(R)$ und $0 \neq p(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$. Setze $d = \text{ggT}\{a_0, \ldots, a_n\}$ (d existiert weil R faktoriell ist wegen Proposition 6.6). Schreibe $p(x) = dq(x)$ (für ein geeignetes $q(x) \in R[x]$). Der ggT der Koeffizienten von q ist nun 1.
Da R faktoriell ist lässt sich d in R als Produkt $d = d_1 \cdots d_m$ von Irreduziblen faktorisieren und diese Irreduziblen in R sind auch in $R[x]$ irreduzibel (Beweis Lemma 7.1 $(**)$).
Nun wollen wir $q(x)$ als Produkt von irreduziblen Polynomen aus $R[x]$ schreiben. Da $F[x]$ faktoriell ist (Beispiel 5.7(ii)), existieren $q_1(x), q_2(x), \ldots, q_n(x) \in F[x]$, irreduzibel in $F[x]$ mit $q(x) = q_1(x) \cdots q_n(x)$. Nach dem Lemma von Gauß können wir annehmen dass $q_i \in R[x]$ für alle $i = 1, \cdots, n$. Da der ggT der Koeffizienten von $q(x)$ 1 ist, ist der ggT der Koeffizienten von q_i auch 1 , für alle $i = 1, \cdots, n$. Nach Korollar 7.4 ist q_i irreduzibel in $R[x]$, für alle $i = 1, \cdots, n$. Wir können also $p(x)$ als Produkt von irreduziblen Polynomen aus $R[x]$ schreiben:
$p(x) = d_1 \cdots d_m q_1(x) \cdots q_n(x)$.
Es bleibt noch zu zeigen, dass diese Faktorisierung eindeutig bis auf Reihenfolge der Faktoren und Multiplikation mit Einheiten ist. Das wird als ÜA gemacht. □

Induktion auf n ergibt:

Korollar 8.2.
Ist R faktoriell so ist $R[x_1, \ldots, x_n]$ auch faktoriell.

Beweis: ÜA.

§ 11 Irreduzibilitätskriterien

Wir untersuchen hier weiter die Irreduzibilität eines Polynoms in einem Integerring. Wir beginnen mit einer Bemerkung:

Bemerkung 8.3. Sei $R = K$ ein Körper, und $0 \neq p(x) \in K[x] \setminus K$. Wenn $\deg p = 1$ dann ist p irreduzibel. Wenn $\deg p = 2$ oder $\deg p = 3$, dann ist p reduzibel genau dann, wenn p einen linearen Faktor in $K[x]$ hat, genau dann, wenn p eine Nullstelle in K hat (s. LA II Skript 4 Korollar 4.1).

Lemma 8.4. Sei $p(x) \in R[x] \setminus R$ ein normiertes Polynom. Dann ist p irreduzible in $R[x]$ genau dann, wenn $p(x)$ kein Produkt $p(x) = a(x)b(x)$ von normierten Polynomen $a(x)$, $b(x)$ mit $\deg a(x) < \deg p(x)$ und $\deg b(x) < \deg p(x)$ ist.

Beweis:
Sei $p(x) \in R[x]$ nicht-konstant, so dass $p(x) = a(x)b(x)$ mit $\deg a(x) < \deg p(x)$ und $\deg b(x) < \deg p(x)$. Da R integer ist, ist $\deg p(x) = \deg a(x) + \deg b(x)$ (s. Beweis Satz 4.8). Da $\deg p(x) > 0$, sind $\deg a(x) > 0$ und $\deg a(x) > 0$, also sind $a(x) \notin R$ und $b(x) \notin R$. Da $R[x]^\times = R^\times$ (s. Beweis Lemma 7.1 $(**)$) sind insbesondere $a(x) \notin R[x]^\times$ und $b(x) \notin R[x]^\times$. Also ist $p(x)$ reduzibel.

Umgekehrt sei $p(x)$ nicht-konstant, normiert und reduzibel in $R[x]$.
Also gibt es Polynome $a'(x) \in R[x] \setminus R[x]^\times$ und $b'(x) \setminus R[x]^\times$ mit $p(x) = a'(x)b'(x)$. Insbesondere sind $a'(x) \notin R^\times$ und $b'(x) \notin R^\times$. Wir bemerken dass der Leitkoeffizient von $p = 1 = a_m b_n$, wobei $a_m \in R$ der Leitkoeffizient von $a'(x)$ und $b_n \in R$ der Leitkoeffizient von $b'(x)$ sind (s. Beweis Satz 4.8). Also sind $a_m, b_n \in R^\times$ (es gelten $b_n = a_m^{-1}$ und $a_m = b_n^{-1}$). Es folgt dass $a'(x) \notin R$ (sonst wäre $a'(x) = a_m \in R^\times$) und analog $b'(x) \notin R$. Also sind $\deg a'(x) < \deg p(x)$ und $\deg b'(x) < \deg p(x)$.

Nun setze $a(x) := a_m^{-1} a'(x)$ und $b(x) := b_n^{-1} b'(x)$. Dann sind $a(x)$ und $b(x)$ normiert mit $\deg a(x) < \deg p(x)$ und $\deg b(x) < \deg p(x)$. Ferner gilt

$$p(x) = a_m b_n p(x) = b_n^{-1} a_m^{-1} a'(x) b'(x) = a_m^{-1} a'(x) b_n^{-1} b'(x) = a(x)b(x).$$

□

Proposition 8.5.
Sei I ein echtes Ideal in R und sei $p(x)$ ein normiertes Polynom aus $R[x] \setminus R$. Wenn $\varphi(p) = \overline{p}(x)$ in $(R/I)[x]$ sich nicht als Produkt $\overline{p}(x) = \overline{a}(x)\overline{b}(x)$ von Polynomen in $(R/I)[x]$ mit $\deg \overline{a}(x) < \deg \overline{p}(x)$ und $\deg \overline{b}(x) < \deg \overline{p}(x)$ darstellen lässt, dann ist $p(x)$ irreduzibel in $R[x]$.

Beweis:
Sei $p(x) \in R[x]$ nicht-konstant, normiert und reduzibel. Aus Lemma 8.4 ist $p(x) = a(x)b(x)$, $a(x)$, $b(x) \in R[x]$ normiert und nicht-konstant. Seien $\overline{p}(x), \overline{a}(x)$ und $\overline{b}(x)$ die Bilder von $p(x), a(x)$ und $b(x)$ in $(R/I)[x]$ (s. Beweis Lemma 7.2). Dann $\overline{p}(x) = \overline{a}(x)\overline{b}(x)$. Da I echt ist, $a(x)$ und $b(x)$ normiert und nicht-konstant sind, so sind auch $\overline{a}(x)$ und $\overline{b}(x)$. Es folgt, dass $\deg \overline{a}(x) < \deg \overline{p}(x)$ und $\deg \overline{b}(x) < \deg \overline{p}(x)$. □

Proposition 8.5 kann man anwenden um zu prüfen ob ein Polynom über $\mathbb{Z}$ irreduzibel ist.

Beispiel:
Betrachte das Polynom $x^4 + 9x^3 + 10x^2 + 22x + 1 \in \mathbb{Z}[x]$.
Das Bild in $\mathbb{Z}_2[x]$ ist $x^4 + x^3 + 1$. Dieses Polynom besitzt keine Nullstelle in $\mathbb{Z}_2$ (prüfe 0 und 1). Daher, wenn es reduzibel ist, dann zerfällt es als Produkt zweier irreduziblen Polynomen aus $\mathbb{Z}_2[x]$ von Grad 2. (Wir arbeiten über $\mathbb{Z}_2 = \mathbb{F}_2$ und können Bemerkung 8.3 ausnutzen). Wenn $p(x) \in \mathbb{Z}_2[x]$ irreduzibel von Grad 2 ist, dann ist das Leitkoeffizient 1 und das konstante Koeffizient ist auch 1 (weil 0 keine Nullstelle ist). Das Polynom x^2+1 hat die Nullstelle 1. Somit gibt es nur ein irreduzibles Polynom von Grad 2 aus $\mathbb{Z}_2[x]$, und zwar $x^2 + x + 1$ (prüfe, dass 0 und 1 keine Nullstelle sind). Aber $(x^2 + x + 1)^2 = x^4 + x^2 + 1$. Somit ist $x^4 + x^3 + 1$ irreduzibel über $\mathbb{Z}_2$ und, daher ist $x^4 + 9x^3 + 10x^2 + 22x + 1$ irreduzibel über $\mathbb{Z}$.

Leider funktioniert dieses Verfahren nicht immer.

Bemerkung 8.6. Seien $a(x), b(x)$ nicht-konstante Polynome $\in R[x]$ so dass $f(x) := a(x)b(x) = x^n$ für ein $n \in \mathbb{N}$. Dann sind $a(x)$ und $b(x)$ Monome, das heißt, es gibt $\alpha, \beta \in R^\times$ und $p, q \in \mathbb{N}$ so dass $a(x) = \alpha x^p$ und $a(x) = \beta x^q$ (und $\alpha\beta = 1$, $p + q = n$). In der Tat kann man zeigen, dass nur die Leitkoeffiziente von $a(x)$ und $b(x)$ ungleich Null sind. Siehe ÜA.

Hier zeigen wir dass die konstante Koeffiziente gleich Null sind. Bemerke dass der konstante Koeffizient $f(0)$ von $f(x) := a(x)b(x)$ das Produkt der konstante Koeffiziente $a(0)$ und $b(0)$ von $a(x)$ and $b(x)$ ist. Wir behaupten dass $b(0) = a(0) = 0$. In der Tat, $0 = f(0) = a(0)b(0)$. Da R ein Integritätsbereich ist, gilt $a(0) = 0$ oder $b(0) = 0$. Angenommen $a(0) = 0$. Sei $F = \text{Quot}\,(R)$ und $m \in \mathbb{N}$ maximal mit $a(x) = x^m a'(x)$ für gewisses $a'(x) \in F[x]$ (m ist die Vielfachheit der Nullstelle $x = 0$ von $a(x)$). Dann $a'(0) \neq 0$ und somit $a'(x)b(x) = x^{n-m}$. Da $b(x)$ nicht konstant ist, dann gilt $n - m > 0$. Daher $a'(0)b(0) = 0$ also $b(0) = 0$ und die Behauptung wurde bewiesen.

Proposition 8.7. (Eisensteinkriterium)
Seien P ein Primideal in R, $n \in \mathbb{N}$ und $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in R[x]$. Angenommen $a_{n-1}, \ldots, a_0 \in P$ aber $a_0 \notin P^2$. Dann ist $f(x)$ irreduzibel in $R[x]$.

Beweis:
Angenommen $f(x) = a(x)b(x)$ in $R[x]$ wobei $a(x)$ und $b(x)$ nicht-konstante normierte Polynome sind (s. Lemma 8.4).
Seien $\overline{f}(x), \overline{a}(x), \overline{b}(x)$ die Bilder von $f(x), a(x)$ bzw. $b(x)$ in $(R/P)[x]$ (s. Beweis Lemma 7.2). Also $x^n = \overline{f}(x) = \overline{a}(x)\overline{b}(x)$. Dann gilt $\overline{a}(0) = \overline{b}(0) = 0$ (man kann Bemerkung 8.6 anwenden weil R/P ein Integerring ist). Aber dann liegen die konstante Koeffizienten von $a(x)$ und $b(x)$ in P und somit liegt der konstante Koeffizient a_0 von $f(x)$ in P^2. Widerspruch. Somit ist $f(x)$ irreduzibel. □

Korollar 8.8.
Sei p prim in $\mathbb{Z}$, $n \geq 1$ und sei $f(x) := x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$. Angenommen p teilt a_i für alle $0 \leq i \leq n-1$ aber p^2 teilt nicht a_0. Dann ist $f(x)$ irreduzibel in $\mathbb{Z}[x]$ sowie in $\mathbb{Q}[x]$.

Beweis:
Für $\mathbb{Z}[x]$: Wende das Eisensteinkriterium auf das Primideal $< p >$ an. Für $\mathbb{Q}[x]$: Korollar 7.4 zu Gauß Lemma anwenden. □

Beispiel:

1. Das Polynom $x^5 + 10x^4 + 25x^2 + 35 \in \mathbb{Z}[x]$ ist irreduzibel nach Eisensteinkriterium auf $p = 5$ angewandt.

2. Sei $f(x) := x^4 + 1 \in \mathbb{Z}[x]$. Wir dürfen das Eisensteinkriterium nicht direkt anwenden. Sei $g(x) = f(x + 1)$, also $g(x) = x^4 + 4x^3 + 6x^2 + 4x + 2$. Nun, nach Eisenstein angewandt auf 2, ist $g(x)$ irreduzibel und, wenn f als Produkt von nicht-konstanten Faktoren zerfällt, dann auch g. Daher ist f irreduzibel.